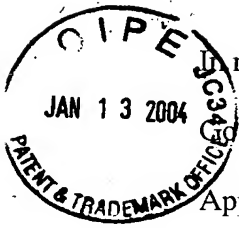


PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE



re application of

Docket No: Q77148

SHIROUZU

Appln. No.: 10/647,442

Group Art Unit: Not Yet Assigned

Confirmation No.: 1641

Examiner: Not Yet Assigned

Filed: August 26, 2003

For: RECORDING METHOD, RECORDING SYSTEM, AND REPRODUCING SYSTEM
OF ENCRYPTION DATA

SUBMISSION OF PRIORITY DOCUMENT

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Submitted herewith is one (1) certified copy of the priority document on which a claim to priority was made under 35 U.S.C. § 119. The Examiner is respectfully requested to acknowledge receipt of said priority document.

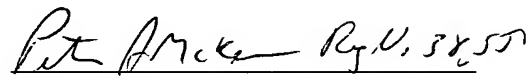
Respectfully submitted,

SUGHRUE MION, PLLC
Telephone: (202) 293-7060
Facsimile: (202) 293-7860

WASHINGTON OFFICE

23373

CUSTOMER NUMBER

for 
Darryl Mexic
Registration No. 23,063

Enclosures: Japan 2002-247127

Date: January 13, 2004

日 本 国 特 許
JAPAN PATENT OFFICE

Go SHIROUZU
USSN: 10/647,442
RECORDING METHOD, RECORDING
SYSTEM
Darryl Mexic 202-663-7909
1 of 1

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日
Date of Application:

2002年 8月27日

出 願 番 号
Application Number:

特願2002-247127

[ST.10/C]:

[JP2002-247127]

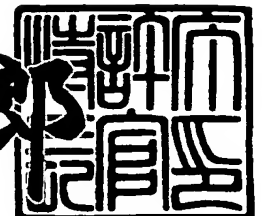
出 願 人
Applicant(s):

富士写真フイルム株式会社

2003年 4月 1日

特 許 庁 長 官
Commissioner,
Japan Patent Office

太田信一郎



出証番号 出証特2003-3023024

【書類名】 特許願

【整理番号】 0207072

【提出日】 平成14年 8月27日

【あて先】 特許庁長官 殿

【国際特許分類】 G11K 15/00
G11B 15/68

【発明者】

 【住所又は居所】 神奈川県小田原市扇町2丁目12番1号
富士写真フイルム株式会社内

 【氏名】 白水 豪

【特許出願人】

 【識別番号】 000005201

 【氏名又は名称】 富士写真フイルム株式会社

【代理人】

 【識別番号】 100064414

 【弁理士】

 【氏名又は名称】 磯野 道造

 【電話番号】 03-5211-2488

【手数料の表示】

 【予納台帳番号】 015392

 【納付金額】 21,000円

【提出物件の目録】

 【物件名】 明細書 1

 【物件名】 図面 1

 【物件名】 要約書 1

 【包括委任状番号】 0016369

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 暗号化データ記録方法、暗号化データ記録システム及び暗号化データ再生システム

【特許請求の範囲】

【請求項 1】 複数の記録媒体を備えるデータ記録システムを使用して、これら記録媒体のうち少なくとも 1 つの記録媒体に暗号化データを書き込むデータ書込ステップと、前記暗号化データのキーデータを複数のキーデータ要素に分割するキーデータ分割ステップと、分割した各キーデータ要素を複数の記録媒体に分けて格納するキーデータ要素格納ステップとを備えることを特徴とする暗号化データ記録方法。

【請求項 2】 複数の記録媒体を備えるデータ記録システムを使用して、これら記録媒体のうち一部の記録媒体に暗号化データを書き込むデータ書込ステップと、前記暗号化データのキーデータを他の記録媒体のいずれか 1 つに格納するキーデータ格納ステップとを備えることを特徴とする暗号化データ記録方法。

【請求項 3】 複数の記録媒体と、前記記録媒体に暗号化データを書き込むドライブと、前記記録媒体のそれぞれに設けられるとともに、前記暗号化データのキーデータが分割されたキーデータ要素を格納するキーデータ要素格納部と、前記暗号化データを生成するとともに、前記ドライブで前記複数の記録媒体のうち少なくとも 1 つの記録媒体に前記暗号化データを書き込ませる手順及び前記暗号化データのキーデータを分割して複数のキーデータ要素を生成するとともに、分割した各キーデータ要素を複数の記録媒体の各キーデータ要素格納部に分けて格納させる手順を実行する制御機構とを備えることを特徴とする暗号化データ記録システム。

【請求項 4】 複数の記録媒体と、前記記録媒体から暗号化データを読み出すドライブと、前記記録媒体のそれぞれに設けられるとともに、前記暗号化データのキーデータが分割されたキーデータ要素を格納するキーデータ要素格納部と、前記ドライブで前記記録媒体に書き込まれた前記暗号化データを読み出させるとともに、前記各キーデータ要素格納部に分けて格納された前記キーデータ要素の全てを読み出させる手順及びこの読み出されたキーデータ要素をもとに前記キ

ーデータを生成するとともに、このキーデータを使用して前記暗号化データを復号化する手順を実行する制御機構とを備えることを特徴とする暗号化データ再生システム。

【請求項5】 複数の記録媒体と、前記記録媒体に暗号化データを書き込むドライブと、前記記録媒体のそれぞれに設けられるとともに、前記暗号化データのキーデータを格納するキーデータ格納部と、前記暗号化データを生成するとともに、前記ドライブで前記複数ある記録媒体のうち一部の記録媒体に前記暗号化データを書き込ませる手順及び前記キーデータを他の記録媒体のいずれか1つの記録媒体の前記キーデータ格納部に格納させる手順を実行する制御機構とを備えることを特徴とする暗号化データ記録システム。

【請求項6】 複数ある記録媒体のうち一部の記録媒体に記録された暗号化データを、他の記録媒体のいずれか1つに格納されたキーデータを使用して再生する暗号化データ再生システムであって、

前記記録媒体から暗号化データを読み出すドライブと、前記記録媒体に設けられるとともに、前記暗号化データのキーデータを格納するキーデータ格納部と、前記ドライブで前記記録媒体に書き込まれた前記暗号化データを読み出させるとともに、前記キーデータ格納部に格納されたキーデータを読み出させる手順及びこのキーデータを使用して前記暗号化データを復号化する手順を実行する制御機構とを備えることを特徴とする暗号化データ再生システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、例えば、磁気テープカートリッジやフレキシブルディスク、光ディスク、リールに巻回された磁気テープ等の可搬性記録媒体に記録されたデータの機密保持技術に関し、特に、複数の可搬性記録媒体を有するデータ記録再生システムでのデータの機密保持技術、さらに詳しくは暗号化データ記録方法、暗号化データ記録システム及び暗号化データ再生システムに関する。

【0002】

【従来技術】

従来、大型コンピュータシステムの外部記憶装置として、多数の磁気テープカートリッジを内蔵するライブラリ装置が広く知られている（例えば、特許文献1、特許文献2及び特許文献3参照）。このライブラリ装置によれば、マガジンに装着された磁気テープカートリッジは、ロボットアームによってマガジンから掴み出されてドライブに搬送されるとともに、ドライブでデータの記録・再生が行われる。そして、このライブラリ装置では、磁気テープカートリッジがマガジンから容易に取り外せることから、例えば、磁気テープカートリッジの盗難等によるデータの漏洩が懸念される。したがって、磁気テープカートリッジに記録されるデータの厳重なセキュリティ管理が望まれる。

【0003】

一般に、データのセキュリティ管理技術として、記録するデータを暗号化する方法が知られている（例えば、特許文献4参照）。この方法では、キーデータを用いる所定のアルゴリズムによって生成した暗号化データを磁気テープといった記録媒体に記録するとともに、記録された暗号化データを再生する際には、前記キーデータを用いてこれを復号化する。

そこで、ライブラリ装置の磁気テープカートリッジに暗号化データを記録しておけば、たとえ磁気テープカートリッジが盗難されたとしても、キーデータが知られることがない限り、その磁気テープカートリッジからのデータの漏洩は免れる。

【0004】

【特許文献1】

特表2002-505787号公報（第16頁Fig1参照）

【0005】

【特許文献2】

特開2002-189994号公報（第11頁右欄第6行～第13頁右欄下から9行目、第21頁図11及び第22頁図12参照）

【0006】

【特許文献3】

特表2001-523877号公報（第66頁第4図参照）

【0 0 0 7】

【特許文献4】

特開昭54-87072号公報（第10頁～第27頁、第1図～第19図参照）

【0 0 0 8】

【発明が解決しようとする課題】

しかしながら、その一方で、データを暗号化する方法では、キーデータを知ることができる者であれば誰でも暗号化データを復号化することができるので、データの機密保持性を高めるとともに、正当な記録媒体へのアクセス権を有する者が容易にデータを利用することができるようにするためには、キーデータの保存をはじめとするキーデータ管理に煩雑を極める。

【0 0 0 9】

そこで、本発明は、キーデータの取り扱いに特段の管理を要することもなく、データの機密保持性が優れ、しかも正当なアクセス権を有する者が容易にデータを利用することができる暗号化データ記録方法、暗号化データ記録システム及び暗号化データ再生システムを提供することを課題とする。

【0 0 1 0】

【課題を解決するための手段】

前記課題を解決するために、請求項1に記載の暗号化データ記録方法は、複数の記録媒体を備えるデータ記録システムを使用して、これら記録媒体のうち少なくとも1つの記録媒体に暗号化データを書き込むデータ書込ステップと、前記暗号化データのキーデータを複数のキーデータ要素に分割するキーデータ分割ステップと、分割した各キーデータ要素を複数の記録媒体に分けて格納するキーデータ要素格納ステップとを備えることを特徴とする。

【0 0 1 1】

この暗号化データ記録方法によれば、複数ある記録媒体のうち少なくとも1つの記録媒体に暗号化データが記録されるとともに、暗号化データの生成に使用されたキーデータは、複数のキーデータ要素に分割されて複数の記録媒体に分けて格納される。

【 0 0 1 2 】

また、この暗号化データ記録方法で記録した暗号化データを再生するに際しては、複数ある記録媒体のうち少なくとも1つの記録媒体に書き込まれた暗号化データを読み出すデータ読出ステップと、前記暗号化データのキーデータを分割して得た複数のキーデータ要素が分けて格納される前記記録媒体から全ての前記キーデータ要素を読み出すキーデータ要素読出ステップと、前記キーデータ要素をもとにキーデータを生成するとともに、このキーデータを使用して、前記暗号化データを復号化する復号化ステップとを備える暗号化データ再生方法が使用される。この暗号化データ再生方法によって、前記記録媒体に分けて格納されたキーデータ要素は、繋ぎ合わせられて再びキーデータに変換されるとともに、このキーデータで暗号化データが復号化される。

【 0 0 1 3 】

したがって、この暗号化データ記録方法は、暗号化データに対して正当なアクセス権を有する者が容易に暗号化データを利用することができ、しかも、暗号化データが記録された記録媒体が例え盗難されたとしても、キーデータを生成するためのキーデータ要素は、複数の記録媒体に分けて格納されており、暗号化データが復号化されることはないので、データの機密保持性が優れる。

また、この暗号化データ記録方法では、キーデータを分割して記録媒体に記録するので、キーデータの鍵長が長い、高度な暗号をも使用することができる。

【 0 0 1 4 】

請求項2に記載の暗号化データ記録方法は、複数の記録媒体を備えるデータ記録システムを使用して、これら記録媒体のうち一部の記録媒体に暗号化データを書き込むデータ書込ステップと、前記暗号化データのキーデータを他の記録媒体のいずれか1つに格納するキーデータ格納ステップとを備えることを特徴とする。

【 0 0 1 5 】

この暗号化データ記録方法では、暗号化データの生成に使用されたキーデータは、暗号化データが記録された記録媒体以外の記録媒体に格納される。

また、この暗号化データ記録方法で記録した暗号データを再生するに際しては

、複数ある記録媒体うち一部の記録媒体に書き込まれた暗号化データを読み出すデータ読出ステップと、前記暗号化データのキーデータが格納された他の記録媒体のいずれか1つの記録媒体から前記キーデータを読み出すとともに、このキーデータを使用して、前記暗号化データを復号化する復号化ステップとを備える暗号化データ再生方法が使用される。

【0016】

したがって、この暗号化データ記録方法は、請求項1の発明と同様に、暗号化データに対して正当なアクセス権を有する者が容易に暗号化データを利用することができ、しかも、暗号化データが記録された記録媒体が例え盗難されたとしても、暗号化データを復号化するキーデータが他の記録媒体に格納されているので、暗号化データが復号化されることはなく、データの機密保持性が優れる。

【0017】

請求項3に記載の暗号化データ記録システムは、複数の記録媒体と、前記記録媒体に暗号化データを書き込むドライブと、前記記録媒体のそれぞれに設けられるとともに、前記暗号化データのキーデータが分割されたキーデータ要素を格納するキーデータ要素格納部と、前記暗号化データを生成するとともに、前記ドライブで前記複数の記録媒体のうち少なくとも1つの記録媒体に前記暗号化データを書き込ませる手順及び前記暗号化データのキーデータを分割して複数のキーデータ要素を生成するとともに、分割した各キーデータ要素を複数の記録媒体の各キーデータ要素格納部に分けて格納させる手順を実行する制御機構とを備えることを特徴とする。

【0018】

この暗号化データ記録システムによれば、制御機構が暗号化データを生成したキーデータを複数のキーデータ要素に分割するとともに、分割したキーデータ要素を複数のキーデータ要素格納部に分けて格納するので、キーデータを構成するキーデータ要素の全てが、暗号化データが記録された記録媒体に格納されることはない。したがって、暗号化データが記録された記録媒体がたとえ盗難されたとしても、暗号化データが復号化されることはないので、本発明の暗号化データ記録システムはデータの機密保持性に優れる。

また、この暗号化データ記録システムでは、キーデータが分割されたキーデータ要素を複数のキーデータ要素格納部に分けて格納するので、キーデータの鍵長が長い、高度な暗号をも使用することができる。

【 0 0 1 9 】

請求項 4 に記載の暗号化データ再生システムは、複数の記録媒体と、前記記録媒体から暗号化データを読み出すドライブと、前記記録媒体のそれぞれに設けられるとともに、前記暗号化データのキーデータが分割されたキーデータ要素を格納するキーデータ要素格納部と、前記ドライブで前記記録媒体に書き込まれた前記暗号化データを読み出させるとともに、前記各キーデータ要素格納部に分けて格納された前記キーデータ要素の全てを読み出させる手順及びこの読み出されたキーデータ要素をもとに前記キーデータを生成するとともに、このキーデータを使用して前記暗号化データを復号化する手順を実行する制御機構とを備えることを特徴とする。

【 0 0 2 0 】

この暗号化データ再生システムによれば、制御機構は、キーデータ要素格納部に格納されたキーデータ要素の全てを読み出して、これを繋ぎ合わせてキーデータを生成するとともに、このキーデータを使用して暗号化データを復号化するので、このシステムの使用者は、煩雑なキーデータの管理を行わなくとも、データの機密保持性を維持しつつ、容易に暗号化データを復号化して利用することができる。

【 0 0 2 1 】

請求項 5 に記載の暗号化データ記録システムは、複数の記録媒体と、前記記録媒体に暗号化データを書き込むドライブと、前記記録媒体のそれぞれに設けられるとともに、前記暗号化データのキーデータを格納するキーデータ格納部と、前記暗号化データを生成するとともに、前記ドライブで前記複数ある記録媒体のうち一部の記録媒体に前記暗号化データを書き込ませる手順及び前記キーデータを他の記録媒体のいずれか 1 つの記録媒体の前記キーデータ格納部に格納させる手順を実行する制御機構とを備えることを特徴とする。

【 0 0 2 2 】

この暗号化データ記録システムによれば、制御機構が、暗号化データを書き込む記録媒体とは異なった記録媒体にキーデータを格納するので、暗号化データが記録された記録媒体がたとえ盗難されたとしても、暗号データが復号化されることはないので、本発明の暗号化データ記録システムはデータの機密保持性に優れる。

【0023】

請求項6に記載の暗号化データ再生システムは、複数ある記録媒体のうち一部の記録媒体に記録された暗号化データを、他の記録媒体のいずれか1つに格納されたキーデータを使用して再生する暗号化データ再生システムであって、前記記録媒体から暗号化データを読み出すドライブと、前記記録媒体に設けられるとともに、前記暗号化データのキーデータを格納するキーデータ格納部と、前記ドライブで前記記録媒体に書き込まれた前記暗号化データを読み出させるとともに、前記キーデータ格納部に格納されたキーデータを読み出させる手順及びこのキーデータを使用して前記暗号化データを復号化する手順を実行する制御機構とを備えることを特徴とする。

【0024】

この暗号化データ再生システムによれば、制御機構は、キーデータ格納部に格納されたキーデータを読み出すとともに、このキーデータを使用して暗号化データを復号化するので、このシステムの使用者は、煩雑なキーデータの管理を行わなくとも、データの機密保持性を維持しつつ、容易に暗号化データを復号化して利用することができる。

【0025】

【発明の実施の形態】

次に、本発明の実施の形態について適宜図面を参照しながら説明する。

図1は、本発明の暗号化データ記録・再生システムの一実施形態として例示するライブラリ装置を備えたコンピュータシステムの構造を概略的に示すブロック図である。

【0026】

図1に示すように、このコンピュータシステム11（以下、単に「システム」

という場合がある) は、ホストコンピュータ等の中央演算処理装置 1 2、この中央演算処理装置 1 2 に接続されるキーボード等の入力装置 1 3 及びライブラリ装置 1 4 を備えている。このシステム 1 1 は、このシステム 1 1 の使用者が入力装置 1 3 から入力するコマンドに応じて中央演算処理装置 1 2 から出力されるデータがライブラリ装置 1 4 内で暗号化されて磁気テープカートリッジ MC に保存されるとともに、この磁気テープカートリッジ MC に保存された暗号化データが復号化されて中央演算処理装置 1 2 で利用されるように構成されている。ここでは、はじめにライブラリ装置 1 4 について説明し、次いでこのライブラリ装置 1 4 を使用した暗号化データ記録方法及び再生方法について説明する。

【 0 0 2 7 】

<ライブラリ装置>

図 2 は、ライブラリ装置の構成を例示する斜視図、図 3 は、アレイに装着された磁気テープカートリッジの様子を示した、一部に切欠き部を含む部分斜視図、図 4 は、磁気テープカートリッジに搭載されるカートリッジメモリの構造を例示する斜視図である。

【 0 0 2 8 】

ライブラリ装置 1 4 は、図 2 に示すように、複数のアレイ 1 5 のそれぞれに着脱自在に装着された磁気テープカートリッジ MC と、磁気テープカートリッジ MC の磁気テープに対して暗号化データの記録・再生を行うドライブ 1 7 と、アレイ 1 5 及びドライブ 1 7 間で磁気テープカートリッジ MC を搬送する搬送機構 1 8 と、ドライブ 1 7 での暗号化データの記録・再生及び搬送機構 1 8 の搬送動作を制御する制御機構 1 9 とを備えている。これらアレイ 1 5、ドライブ 1 7、搬送機構 1 8 及び制御機構 1 9 は、透明パネル 2 1 が嵌め込まれた扉 2 2 を有するケース 2 3 内に収納されている。

【 0 0 2 9 】

アレイ 1 5 は、後記する磁気テープカートリッジ MC を載置する底板 2 4 と、この底板 2 4 から垂直に立ち上がり、底板 2 4 を 3 方から取り囲む側板 2 5 とを備えており、側板 2 5 の無いアレイ 1 5 前方から磁気テープカートリッジ MC が装着されるようになっているとともに、側板 2 5 で磁気テープカートリッジ MC

の横方法への動きが制止されるようになっている。本実施の形態では、複数の磁気テープカートリッジMCが収納できるように、アレイ15がケース23内に配置された支持台26上に複数段積み上げられるとともに、複数列配列されている。

【0030】

ドライブ17は、公知のものを使用することができ、本実施の形態では、図2に示すように、3基のドライブ17がケース23内に積み重ねられている。

搬送機構18としては、例えば、特表2002-505787号公報、特開2002-189994号公報、特表2001-523877号公報等の開示される公知の搬送機構を使用することができる。本実施の形態では、搬送機構18が、図2に示すように、公知の搬送機構に準じて、ロボットアーム27、レール28、ターンテーブル29及びロボットアーム駆動モータ31で構成されている。

【0031】

ロボットアーム27は、アレイ15に装着された磁気テープカートリッジMCを握持する握持機構（図示せず）を先端に有するとともに、その後端がケース23の床面に配置されたターンテーブル29から垂直に伸びるレール28にロボットアーム駆動モータ31を介して上下動可能に支持されている。そして、ロボットアーム27は、アレイ15から磁気テープカートリッジMCを引き出し、あるいは磁気テープカートリッジMCをアレイ15やドライブ17に押し込むカートリッジ着脱機構（図示せず）を備えている。なお、このような搬送機構18によれば、ロボットアーム27は、ターンテーブル29が回転することによって、所定の回転軸周りに揺動するとともに、ロボットアーム駆動モータ31が駆動することによって、垂直移動する。したがって、ロボットアーム27は、この搬送機構18に向き合う所定のアレイ15に装着される磁気テープカートリッジMCを握持機構で握持し、そしてカートリッジ着脱機構でアレイ15から磁気テープカートリッジMCを引き出すとともに、ターンテーブル29及びロボットアーム駆動モータ31を所定の条件で駆動させれば、磁気テープカートリッジMCをドライブ17に向けて搬送することができる。また、これとは逆に、搬送機構は、ドライブ17に装着された磁気テープカートリッジMCをアレイ15に向けて搬送

し、アレイ 1 5 に磁気テープカートリッジ MC を装着することができる。

【 0 0 3 2 】

ロボットアーム 2 7 は、さらに、アレイ 1 5 (磁気テープカートリッジ MC) と向き合う先端にカートリッジメモリインターフェース 3 2 を備えている。このカートリッジメモリインターフェース 3 2 は、アレイ 1 5 やドライブ 1 7 に装着された、後記する磁気テープカートリッジ MC のカートリッジメモリ CM と所定の距離をおいて遠隔的にデータの授受を行うためのものである。このカートリッジメモリインターフェース 3 2 には、例えば特開 2 0 0 2 - 1 8 9 9 9 4 号公報に開示される公知のものを使用することができる。本実施の形態では、カートリッジメモリインターフェース 3 2 が、公知のものに準じて、ループアンテナとこのループアンテナに接続される変復調器 (ともに図示せず) とで構成されている。

【 0 0 3 3 】

磁気テープカートリッジ MC には、いわゆる L T O 規格に準拠した磁気テープカートリッジが使用されるとともに、図 3 に示すように、カートリッジメモリ CM が搭載されている。

このカートリッジメモリ CM は、後記するデータの暗号化及び復号化に使用されるキーデータが分割されたキーデータ要素及びキーデータ要素が格納されたカートリッジメモリ CM を特定するカートリッジ特定データを格納するものである。なお、カートリッジメモリ CM には、周知のように、製造者や製造番号等の磁気テープカートリッジ MC の製造情報や、使用者や使用日時等の磁気テープカートリッジの使用履歴情報等が記録されてもよい。

このカートリッジメモリ CM の配置位置は、磁気テープ 3 4 の走行に支障をきたすことが無いカートリッジケース 3 5 内の隅で、しかも磁気テープカートリッジ MC がアレイ 1 5 に装着された状態で、アレイ 1 5 前方から突き出した先端近傍に設定されている。

【 0 0 3 4 】

カートリッジメモリ CM は、図 4 に示すように、矩形の薄片形状を有する樹脂製の基板 3 4 と、基板 3 4 上にプリント配線された電磁誘導用のループアンテナ

36と、ループアンテナ36を介して前記したカートリッジメモリインターフェース32との間でデータ（キーデータ等）の授受を行うためのICチップ37とを有している。なお、ICチップ37は樹脂で形成されたグローブトップ38内に封止され保護されている。

【0035】

制御機構19は、図1に示すように、メインコントローラ39、暗号コントローラ40及び搬送コントローラ41からなる制御部42と、メインテーブル43、暗号データテーブル44、キーデータテーブル45及び搬送条件設定テーブル46からなる制御メモリ47とを備えている。

【0036】

メインコントローラ39は、中央演算処理装置12からの命令信号を受けることにより、メインテーブル43に格納されたプログラムに従って、ライブラリ装置14を統括的に制御するものであり、後記する暗号化データ記録方法及び暗号化データ再生方法に示す手順で、暗号コントローラ40、搬送コントローラ41、搬送機構18及びドライブ17の動作を制御するように構成されている。

【0037】

暗号コントローラ40は、磁気テープカートリッジMCに暗号化データを記録するにあたって、後記する暗号化データ記録方法に示す手順で、暗号化前のいわゆる生データを暗号化するのに使用するキーデータを生成し、このキーデータで生データを暗号化し、暗号化データを記録させるべくドライブ17に向けて暗号化データを送信し、そして、キーデータを分割することにより後記するキーデータ要素を生成し、所定のカートリッジメモリCMにキーデータ要素を格納すべくキーデータ要素をカートリッジメモリインターフェース32に向けて送信するように構成されているとともに、磁気テープカートリッジMCに記録された暗号化データを再生するにあたって、後記する暗号化データ再生方法に示す手順で、カートリッジメモリCMに格納されたキーデータ要素をもとにキーデータを生成し、磁気テープカートリッジMCに記録された暗号化データをキーデータで生データに復号化するように構成されている。

【0038】

搬送コントローラ 4 1 は、メインコントローラ 3 9 からの命令信号を受けることにより、搬送条件設定テーブル 4 6 に格納された後記する座標データに基づいて、ロボットアーム 2 7 を移動させるとともに、同じく搬送条件設定テーブル 4 6 に格納されたロボットアーム 2 7 の握持機構及びカートリッジ着脱機構の動作に関わるプログラムに従って、握持機構及びカートリッジ着脱機構を制御するように構成されている。

【0039】

暗号データテーブル 4 4 は、生データ及び暗号化データを一時記憶するように構成されている。

キーデータテーブル 4 5 は、暗号コントローラ 4 0 で生成されたキーデータ及びこのキーデータから生成された後記するキーデータ要素及びキーデータ要素が格納されたカートリッジメモリ CM を特定するための後記するカートリッジメモリ特定データを一時記憶するように構成されている。

搬送条件設定テーブル 4 6 は、ロボットアーム 2 7 が各磁気テープカートリッジ MC 及び各ドライブ 1 7 にアクセスする際の所定の位置を特定する座標データ、並びにロボットアーム 2 7 の握持機構及びカートリッジ着脱機構の動作に関わるプログラムを格納するように構成されている。

【0040】

<暗号化データ記録方法>

次に、前記ライブラリ装置 1 4 を使用した暗号化データ記録方法について説明する。なお、ここでは、図 1 に示すように、第 1 磁気テープカートリッジ MC₁ から第 n 磁気カートリッジ MC_n までの n 個（n は 2 以上の整数）の磁気テープカートリッジ MC と、1 つのドライブ 1 7 とを備えるライブラリ装置 1 4 において、第 k 磁気テープカートリッジ MC_k（但し、 $1 \leq k \leq n$ であり、n は前記と同じ）に暗号化データを記録する場合を例にとって説明する。

【0041】

図 5 は、中央演算処理装置から生データがライブラリ装置に送信されて、キーデータ要素が生成・保存される際のメインコントローラ、暗号コントローラ及び搬送コントローラの動作を例示するフローチャート、図 6（a）は、暗号コント

ローラで生成されるキーデータ要素のデータ構造を示す概念図、図 6 (b) は、キーデータテーブルに格納されるキーデータ要素のデータ構造を示す概念図、図 7 は、カートリッジメモリに格納されるキーデータ要素のデータ構造及びカートリッジ特定データのデータ構造を示す概念図、図 8 は、キーデータを使用して暗号化データを生成する際のメインコントローラ及び暗号コントローラの動作を例示するフローチャートである。なお、図 7 中、CM はカートリッジメモリを表わす。

【 0 0 4 2 】

この暗号データ記録方法では、中央演算処理装置 1 2 からメインコントローラ 3 9 に向けて生データが送信されると、図 5 に示すように、メインコントローラ 3 9 は、暗号コントローラ 4 0 に向けて生データを送信するとともに、この生データを保存するように命令信号を送信する (S 1)。この命令信号を受けた暗号コントローラ 4 0 は、暗号データテーブル 4 4 に生データを保存するとともに (S 2)、保存完了信号をメインコントローラ 3 9 に向けて送信する (S 3)。

メインコントローラ 3 9 は、保存完了信号を受け取ることにより、搬送コントローラ 4 1 に向けて媒体搬送命令を送信する (S 4)。搬送コントローラ 4 1 では、この媒体搬送命令信号を受けて、搬送条件設定テーブル 4 6 に格納された座標データを参照し、アレイ 1 5 に装着された第 k 磁気テープカートリッジ MC_k をドライブ 1 7 まで搬送するように、搬送機構 1 8 に向けて搬送機構駆動命令信号を送信する (S 5)。この搬送機構駆動命令信号を受けた搬送機構 1 8 がドライブ 1 7 への第 k 磁気テープカートリッジ MC_k の装着を完了させると、搬送コントローラ 4 1 は、メインコントローラ 3 9 に向けて搬送完了信号を送信する (S 6)。

【 0 0 4 3 】

メインコントローラ 3 9 は、搬送完了信号を受けると、暗号コントローラ 4 0 に向けてキーデータの生成命令信号を送信する (S 7)。暗号コントローラ 4 0 は、生データを暗号化するキーデータを生成するとともに、このキーデータをキーデータテーブル 4 5 に保存する (S 8)。このキーデータの生成方法は、公知の方法を使用することができ、このような方法としては、例えば特開昭 5 4 - 8

7 0 7 2 号公報に開示する方法が挙げられる。

【0 0 4 4】

次いで、暗号コントローラ 4 0 は、キーデータを分割してキーデータ要素を生成するとともに、このキーデータ要素をキーデータテーブル 4 5 に保存する (S 9)。キーデータの分割数 (X) は、 $X = 2 \sim n$ (n は前記と同じ) の範囲で設定すればよい。なお、本実施の形態では、 $X = n$ の場合、すなわち図 6 (a) に示すように、第 1 磁気テープカートリッジ MC_1 から第 n 磁気テープカートリッジ MC_n までの全てのカートリッジメモリ CM に割り当てるようにキーデータ 4 8 を n 分割して、キーデータ要素 $a_1, a_2 \cdots a_n$ を生成する。そして、暗号コントローラ 4 0 は、キーデータ要素 $a_1, a_2 \cdots a_n$ をキーデータテーブル 4 5 に保存するにあたって、図 6 (b) に示すように、割当先のカートリッジメモリ CM を特定する識別子 $A_1, A_2 \cdots A_n$ を各キーデータ要素 $a_1, a_2 \cdots a_n$ に付加する。したがって、キーデータテーブル 4 5 に保存される各キーデータ要素 $a_1, a_2 \cdots a_n$ には、それぞれ格納先のカートリッジメモリ CM を示す識別子 $A_1, A_2 \cdots A_n$ が付加されることになる。

【0 0 4 5】

ここで再び図 5 を参照すると、所定の識別子付きのキーデータ要素を保存した暗号コントローラ 4 0 は、メインコントローラ 3 9 に向けて、キーデータ要素の保存完了信号を送信する (S 1 0)。

次に、メインコントローラ 3 9、暗号コントローラ 4 0 及び搬送コントローラ 4 1 は、メインコントローラ 3 9 がこの保存完了信号を受けたことをきっかけに、次の S 1 1 ~ S 1 6 のステップ (図 5 中、符号 4 9 で示す) を、キーデータ要素が格納されるカートリッジメモリ CM の数に等しい回数、すなわち n 回繰り返す。

まず、メインコントローラ 3 9 は、ロボットアーム 2 7 の先端に配置されたカートリッジメモリインターフェース 3 2 が所定のカートリッジメモリ CM にアクセスするように、第 1 番目の CM アクセス命令信号を搬送コントローラ 4 1 に向けて送信する (S 1 1)。この CM アクセス命令信号を受けた搬送コントローラ 4 1 は、キーデータテーブル 4 5 (図 1 参照) を参照することにより、キーデー

タテーブル 4 5 に保存された、例えば識別子 A_1 を有するキーデータ要素 a_1 (図 6 (b) 参照) を読み出す。

【 0 0 4 6 】

次いで、搬送コントローラ 4 1 は、識別子 A_1 で特定されるカートリッジメモリ CM、すなわち第 1 磁気テープカートリッジのカートリッジメモリ CM にカートリッジメモリインターフェース 3 2 がアクセスできるようにロボットアーム 2 7 を移動させるための搬送機構駆動命令信号を搬送機構 1 8 に向けて送信する (S 1 2)。搬送機構 1 8 がロボットアーム 2 7 を所定の位置に搬送して、カートリッジメモリインターフェース 3 2 が第 1 磁気テープカートリッジ MC_1 のカートリッジメモリ CM にアクセスすると、搬送コントローラ 4 1 は、メインコントローラ 3 9 に向けて CM アクセス完了信号を送信する (S 1 3)。

【 0 0 4 7 】

この CM アクセス完了信号を受けたメインコントローラ 3 9 は、キーデータ要素 a_1 を第 1 磁気テープカートリッジ MC_1 のカートリッジメモリ CM に格納するようキーデータ要素格納命令信号を暗号コントローラ 4 0 に向けて送信する (S 1 4)。この命令信号を受けた暗号コントローラ 4 0 は、キーデータテーブル 4 5 からキーデータ要素 a_1 を読み出して、カートリッジメモリインターフェース 3 2 (図 1 参照) に送信することにより、キーデータ要素 a_1 を第 1 磁気テープカートリッジ MC_1 のカートリッジメモリ CM に格納する (S 1 5)。なお、カートリッジメモリインターフェース 3 2 に向けて送信されたキーデータ要素 a_1 は、前記したカートリッジメモリインターフェース 3 2 の変復調器、ループアンテナ及びカートリッジメモリ CM のループアンテナ 3 6 を介して IC チップ 3 7 (図 4 参照) に格納される。カートリッジメモリ CM 及びカートリッジメモリインターフェース 3 2 間の通信方式は、例えば特開 2 0 0 2 - 1 8 9 9 9 4 号公報に開示されるような公知の方式でよく、ここでの通信方式の詳細な説明は省略する。

【 0 0 4 8 】

次に、キーデータ要素 a_1 の格納が完了すると、暗号コントローラ 4 0 は、メインコントローラ 3 9 に向けて、キーデータ要素 a_1 の格納完了信号を送信する

(S 1 6)。この完了信号を受けたメインコントローラ 3 9 は、第 2 番目の CM アクセス命令信号を搬送コントローラ 4 1 に向けて送信する (S 1 1)。

この第 2 番目の CM アクセス命令信号を受けた搬送コントローラ 4 1 は、再び キーデータテーブル 4 5 (図 1 参照) を参照することにより、前記識別子 A_1 以外の識別子を有するキーデータ要素、例えば、識別子 A_2 を有するキーデータ要素 a_2 (図 6 (b) 参照) を読み出す。

【0 0 4 9】

次いで、搬送コントローラ 4 1 は、識別子 A_2 で特定されるカートリッジメモリ CM、すなわち第 2 磁気テープカートリッジ MC_2 のカートリッジメモリ CM にカートリッジメモリインターフェース 3 2 がアクセスできるようにロボットアーム 2 7 を移動させるための搬送機構駆動命令信号を搬送機構 1 8 に向けて送信する (S 1 2)。以後、前記したと同様にして、S 1 3 ~ S 1 6 のステップが実行されることにより、キーデータ要素 a_2 が、第 2 磁気テープカートリッジ MC_2 のカートリッジメモリ CM に格納されるとともに、暗号コントローラ 4 0 からメインコントローラ 3 9 に向けてキーデータ要素格納完了信号が送信される。

【0 0 5 0】

本実施の形態では、図 7 に示すように、この一連の S 1 1 ~ S 1 6 のステップが n 回繰り返されることによって、第 1 ~ 第 n 磁気テープカートリッジ MC_1 · · · MC_n のカートリッジメモリ CM には、それぞれキーデータ要素 a_1 , a_2 · · · a_n が格納される。

そして、さらに、暗号コントローラ 4 0 は、図 7 に示すように、キーデータ要素 a_1 , a_2 · · · a_n が格納されたカートリッジメモリ CM を特定するカートリッジ特定データ (P_1 , P_2 · · · P_n) を、暗号化データが書き込まれる第 k 磁気テープカートリッジ MC_k のカートリッジメモリ CM に格納する。このカートリッジ特定データ (P_1 , P_2 · · · P_n) は、後記する暗号化データ再生方法で、キーデータ要素 a_1 , a_2 · · · a_n からキーデータを生成するとき使用するものである。

【0 0 5 1】

そして、暗号コントローラ 4 0 からメインコントローラ 3 9 に向けて、最後の

キーデータ要素、例えば第 n 磁気テープカートリッジ MC_n へのキーデータ要素 a_n の格納完了信号が送信されると(図5参照)、メインコントローラ39は、図8に示すように、暗号コントローラ40に向けて、生データの暗号化命令信号を送信する(S17)。この命令信号を受けた暗号コントローラ40は、前記ステップS2で暗号データテーブル44に保存した生データ及び前記ステップS8でキーデータテーブル45に保存したキーデータを、暗号データテーブル44及びキーデータテーブル45から読み出す(S18)。そして暗号コントローラ40は、読み出したキーデータを使用して生データを暗号化するとともに、暗号化データを暗号データテーブル44に保存する(S19)。この暗号化データの生成方法は、公知の方法を使用することができ、このような方法としては、例えば特開昭54-87072号公報に開示する方法が挙げられる。

【0052】

暗号化データの保存が完了すると、暗号コントローラ40は、メインコントローラ39に向けて暗号化データの保存完了信号を送信する(S20)。メインコントローラ39は、この保存完了信号を受けてドライブ17(図1参照)を駆動させるとともに、暗号コントローラ40に向けて暗号化データの書込命令信号を送信する(S21)。この書込命令信号を受けた暗号コントローラ40は、暗号データテーブル44から暗号データを読み出すとともに、駆動するドライブ17に向けてこの暗号化データを送信する(S22)。この送信によって、ドライブ17での暗号化データの書込みが完了すると、暗号コントローラ40は、暗号データテーブル44及びキーデータテーブル45に保存された生データ、暗号化データ、キーデータ及びキーデータ要素を消去する(S23)。そして、搬送機構18によって第 k 磁気テープカートリッジ MC_k が所定のアレイ15に戻されることによってこの暗号化データ記録方法は終了する。

【0053】

<暗号化データ再生方法>

次に、前記ライブラリ装置を使用した暗号化データ再生方法について説明する。なお、ここでは、前記した暗号化データ記録方法によって第 k 磁気テープカートリッジに記録された暗号化データを復号化する場合を例にとって説明する。

図 9 は、中央演算処理装置から生データを要求する信号がライブラリ装置に送信されて、キーデータ要素をもとにキーデータが生成・保存される際のメインコントローラ、暗号コントローラ及び搬送コントローラの動作を例示するフローチャート、図 1 0 は、暗号化データを生データに復号化する際のメインコントローラ及び暗号コントローラの動作を例示するフローチャートである。

【 0 0 5 4 】

この暗号データ再生方法では、中央演算処理装置 1 2 からメインコントローラ 3 9 に向けて生データを要求する信号が送信されると、図 9 に示すように、メインコントローラ 3 9 は、媒体搬送命令を搬送コントローラ 4 1 に向けて送信する (S 2 4)。搬送コントローラ 4 1 では、この命令信号を受けて、搬送条件設定テーブル 4 6 に格納された座標データを参照することにより、第 k 磁気テープカートリッジ MC_k をドライブ 1 7 まで搬送させるために、搬送機構駆動命令信号を搬送機構 1 8 に向けて送信する (S 2 5)。この搬送機構駆動命令信号を受けた搬送機構 1 8 は、第 k 磁気テープカートリッジ MC_k をドライブ 1 7 に搬送して装着する。なお、このときロボットアーム 2 7 は、ロボットアーム 2 7 の先端に配置されたカートリッジメモリインターフェース 3 2 がカートリッジメモリ CM とアクセスできるように姿勢を維持している。第 k 磁気テープカートリッジ MC_k の搬送が完了すると、搬送コントローラ 4 1 は、メインコントローラ 3 9 に向けて搬送完了信号を送信する (S 2 6)。

【 0 0 5 5 】

メインコントローラ 4 0 は、搬送完了信号を受けると、前記したステップ S 1 5 で格納したカートリッジ特定データ ($P_1, P_2 \cdots P_n$) (図 5 及び図 7 参照) を第 k 磁気テープカートリッジ MC_k のカートリッジメモリ CM から読み出すように、カートリッジ特定データ読出命令信号を暗号コントローラ 4 0 に向けて送信する (S 2 7)。この読出命令信号を受けた暗号コントローラ 4 0 は、カートリッジメモリインターフェース 3 2 を介してカートリッジメモリ CM に格納されたカートリッジ特定データを読み出すとともに、このデータをキーデータテーブル 4 5 に保存する (S 2 8)。そして、カートリッジ特定データの保存が完了すると、暗号コントローラ 4 0 は、メインコントローラ 3 9 に向けて、カー

トリッジ特定データの保存完了信号を送信する（S 2 9）。

【0 0 5 6】

次に、メインコントローラ 3 9、暗号コントローラ 4 0 及び搬送コントローラ 4 1 は、メインコントローラ 3 9 がこの保存完了信号を受けたことをきっかけに、次の S 3 0 ~ S 3 5 のステップ（図 9 中、符号 5 0 で示す）を、カートリッジ特定データで特定されたカートリッジメモリ CM の数に等しい回数、すなわち n 回繰り返す。

【0 0 5 7】

まず、メインコントローラ 3 9 は、ロボットアーム 2 7 の先端に配置されたカートリッジメモリインターフェース 3 2 が特定されたカートリッジメモリ CM の 1 つにアクセスするように第 1 番目の CM アクセス命令信号を搬送コントローラ 4 1 に向けて送信する（S 3 0）。この CM アクセス命令信号を受けた搬送コントローラ 4 1 は、キーデータテーブル 4 5（図 1 参照）を参照することにより、キーデータテーブル 4 5 に保存された、例えばカートリッジ特定データ P_1 を参照する（図 7 参照）。

【0 0 5 8】

次いで、搬送コントローラ 4 1 は、カートリッジ特定データ P_1 で特定されるカートリッジメモリ CM、すなわち第 1 磁気テープカートリッジ MC_1 のカートリッジメモリ CM にロボットアーム 2 7 のカートリッジメモリインターフェース 3 2 がアクセスできるようにロボットアーム 2 7 を移動させるための搬送機構駆動命令信号を搬送機構 1 8 に向けて送信する（S 3 1）。搬送機構 1 8 がロボットアーム 2 7 を所定の位置に移動して、カートリッジメモリインターフェース 3 2 が第 1 磁気テープカートリッジ MC_1 のカートリッジメモリ CM にアクセスすると、搬送コントローラ 4 1 は、メインコントローラ 3 9 に向けて CM アクセス完了信号を送信する（S 3 2）。この CM アクセス完了信号を受けたメインコントローラ 3 9 は、暗号コントローラ 4 0 に向けて、キーデータ要素読出命令を送信する（S 3 3）。この命令信号を受けた暗号コントローラ 4 0 は、第 1 磁気テープカートリッジ MC_1 のカートリッジメモリ CM からカートリッジメモリインターフェース 3 2 を介してキーデータ要素 a_1 を読み出すとともに、このキーデ

ータ要素 a_1 をキーデータテーブル 4 5 に保存する (S 3 4)。なお、キーデータ要素 a_1 は、前記したカートリッジメモリインターフェース 3 2 の変復調器、ループアンテナ及びカートリッジメモリ CM のループアンテナ 3 6 を介して IC チップ 3 7 (図 4 参照) から読み出される。

【 0 0 5 9 】

次に、キーデータ要素 a_1 の読出及び保存が完了すると、暗号コントローラ 4 0 は、メインコントローラ 3 9 に向けて、キーデータ要素の保存完了信号を送信する (S 3 5)。この保存完了信号を受けたメインコントローラ 3 9 は、第 2 番目の CM アクセス命令信号を搬送コントローラ 4 1 に向けて送信する (S 3 0)。

【 0 0 6 0 】

第 2 番目の CM アクセス命令信号を受けた搬送コントローラ 4 1 は、再びキーデータテーブル 4 5 (図 1 参照) を参照することにより、前記カートリッジ特定データ P_1 以外のカートリッジ特定データ、例えば P_2 をキーデータテーブル 4 5 から読み出す。次いで、搬送コントローラ 4 1 は、 P_2 で特定されるカートリッジメモリ CM、すなわち第 2 磁気テープカートリッジ MC_2 のカートリッジメモリ CM にロボットアーム 2 7 のカートリッジメモリインターフェース 3 2 がアクセスできるようにロボットアーム 2 7 を移動させる搬送機構駆動命令信号を搬送機構 1 8 に向けて送信する (S 3 1)。以後、前記したと同様にして、S 3 2 ~ S 3 5 のステップが実行されることにより、キーデータ要素 a_2 が、キーデータテーブル 4 5 に保存されるとともに、キーデータ要素保存完了信号が暗号コントローラ 4 0 からメインコントローラ 3 9 に向けて送信される。本実施の形態では、この一連の S 3 0 ~ S 3 5 のステップが繰り返されることによって、第 1 ~ 第 n 磁気テープカートリッジ $MC_1 \cdots MC_n$ のカートリッジメモリ CM に格納されていたキーデータ要素 $a_1, a_2 \cdots a_n$ は、キーデータテーブル 4 5 に保存される。

【 0 0 6 1 】

そして、最後のキーデータ要素、例えば第 n 磁気テープカートリッジ MC_n のキーデータ要素 a_n のキーデータテーブル 4 5 への保存完了信号が、暗号コント

ローラ 4 0 からメインコントローラ 3 9 に向けて送信されると、メインコントローラ 3 9 は、キーデータの生成命令信号を暗号コントローラ 4 0 に向けて送信する (S 3 6)。この命令信号を受けた暗号コントローラ 4 0 は、キーデータテーブル 4 5 から全てのキーデータ要素 $a_1, a_2 \dots a_n$ を読み出すとともに、これらがもとの順番に配列するように繋ぎ合わせてキーデータを生成し、このキーデータをキーデータテーブル 4 5 に保存する (S 3 7)。キーデータの保存が完了すると、暗号コントローラ 4 0 は、保存完了信号をメインコントローラ 3 9 に向けて送信する (S 3 8)。

【 0 0 6 2 】

メインコントローラ 3 9 は、この保存完了信号を受けると、ドライブ 1 7 を駆動させるとともに、図 1 0 に示すように、暗号化データの読出命令信号を暗号コントローラ 4 0 に向けて送信する (S 3 9)。暗号コントローラ 4 0 は、この命令信号を受けることにより、ドライブ 1 7 に装着された第 k 磁気テープカートリッジ MC_k から暗号化データを読み出し、この暗号化データを暗号データテーブル 4 4 に保存する (S 4 0)。暗号化データの保存が完了すると、暗号コントローラ 4 0 は、暗号化データの保存完了信号をメインコントローラ 3 9 に向けて送信する (S 4 1)。メインコントローラ 3 9 は、この保存完了信号を受けることにより、暗号化データの復号化命令信号を暗号コントローラ 4 0 に向けて送信する (S 4 2)。

【 0 0 6 3 】

暗号コントローラ 4 0 は、復号化命令信号を受けて、前記ステップ S 3 7 でキーデータテーブル 4 5 に保存したキーデータ及び前記ステップ S 4 0 で暗号データテーブル 4 4 に保存した暗号化データを、キーデータテーブル 4 5 及び暗号データテーブル 4 4 から読み出す (S 4 3)。そして暗号コントローラ 4 0 は、読み出したキーデータを使用して暗号化データを復号化することによって生データを生成する (S 4 4) とともに、生データをメインコントローラ 3 9 に向けて送信する (S 4 5)。なお、暗号化データを復号化する方法は、公知の方法を使用することができ、このような方法としては、例えば特開昭 5 4 - 8 7 0 7 2 号公報に開示する方法が挙げられる。

【 0 0 6 4 】

生データの送信が完了すると、暗号コントローラ 4 0 は、暗号データテーブル 4 4 及びキーデータテーブル 4 5 に保存された、暗号化データ、キーデータ、キーデータ要素及びカートリッジ特定データを消去する (S 4 7)。その一方で、メインコントローラ 3 9 は、生データを中央演算処理装置 1 2 に向けて送信する (S 4 6)。そして、搬送機構 1 8 によって第 k 磁気テープカートリッジ MC_k が所定のアレイ 1 5 に戻されてこの暗号化データ再生方法は終了する。

【 0 0 6 5 】

このようなライブラリ装置 1 4、すなわち本発明の暗号化データ記録・再生システム並びにこのシステムを使用した暗号化データ記録方法及び暗号化データ再生方法によれば、中央演算処理装置 1 2 から送信された生データが、キーデータで暗号化データに変換されるとともに、複数ある磁気テープカートリッジ MC のうち、少なくとも 1 つの磁気テープカートリッジ MC にこの暗号化データが記録され、しかも、データの暗号化に使用されたキーデータは、複数のキーデータ要素に分割されて複数のカートリッジメモリ CM に分けて格納される。

【 0 0 6 6 】

そして、磁気テープカートリッジ MC に記録された暗号化データを再生する際には、分けて格納されたキーデータ要素を繋ぎ合わせて再びキーデータに変換するとともに、このキーデータで暗号化データが復号化される。

したがって、暗号化データ記録・再生システムに対して正当なアクセス権を有する者は、容易に暗号化データを利用することができ、しかも、暗号化データが記録された磁気テープカートリッジ MC が、例え盗難されたとしても、キーデータを生成するためのキーデータ要素は、複数のカートリッジメモリ CM に分けて格納されており、暗号化データが復号化されることはないので、データの機密保持性が優れる。

【 0 0 6 7 】

また、キーデータ要素からキーデータを生成する際に必要な、各キーデータ要素の格納先を特定するためのカートリッジ特定データは、ライブラリ装置 1 4 内における各磁気テープカートリッジ MC の配置位置と、この位置座標データを格

納する搬送設定条件テーブル46とに関連付けられている。すなわち、カートリッジ特定データは、ライブラリ装置14固有のデータであるので、ライブラリ装置14の全ての磁気テープカートリッジMCが盗難され、そして暗号データが保存されている磁気テープカートリッジMCのカートリッジメモリCMからカートリッジ特定データを取得しえたとしても、キーデータを生成するために必要なキーデータ要素とそれを格納する磁気テープカートリッジMCとの対応付けができないため、キーデータを生成することはできない。したがって、暗号データが復号化されることはない。

【0068】

そしてまた、キーデータ要素の格納部には、磁気テープカートリッジMCのカートリッジメモリCMが使用されるとともに、カートリッジメモリCMに対するキーデータの書込み及び読出しには、カートリッジメモリCMとの間で非接触でキーデータ要素の授受を行うカートリッジメモリインターフェース32が使用されている。そして、カートリッジメモリインターフェース32が、ロボットアーム27の先端に配置されているので、ロボットアーム27を磁気テープカートリッジMCに近接させるだけでキーデータ要素の授受を行うことができる。したがって、例えばドライブ17を使用して磁気テープのヘッダ部分にキーデータ要素を書込みあるいはそのヘッダ部分から読み出す場合に比べて、キーデータ要素の書込み及び読出しが速やかに行われる。

【0069】

さらに、この暗号化データ記録・再生システム並びにこのシステムを使用した暗号化データ記録方法及び暗号化データ再生方法によれば、キーデータが分割されたキーデータ要素を格納するので、比較的格納容量の少ないカートリッジメモリCM（数キロバイト程度）を使用する場合にあっても、キーデータの鍵長が長い、高度な暗号をも使用することができる。

【0070】

以上、詳述した本実施の形態では、キーデータをカートリッジメモリCMの数に等しい数、すなわち n 個に分割してキーデータ要素を生成するとともに、第1～第 n 磁気テープカートリッジMC₁・・・MC _{n} のカートリッジメモリCMの

全てに、キーデータ要素を割り当てて格納したが、本発明は、これに制限されるものではなく、暗号化データが記録される第 k 磁気テープカートリッジ MC_k のカートリッジメモリ CM にキーデータが格納されていなければよい。

【0071】

したがって、例えば、前記したキーデータの分割数(X)は、カートリッジメモリ CM の数より少ない数に設定してもよい。この場合、キーデータ要素は、暗号化データが記録される第 k 磁気テープカートリッジ MC_k のカートリッジメモリ CM に格納されても、格納されなくともよい。また1つのカートリッジメモリ CM に対して、複数のキーデータ要素が格納されてもよい。このようにキーデータの分割数(X)を、カートリッジメモリ CM の数より少ない数に設定した暗号データ記録・再生方法及び暗号データ記録・再生システムでは、前記したステップ $S11 \sim S16$ (図5中、符号49参照)及びステップ $S20 \sim S35$ (図9中、符号50参照)の繰返し回数を、キーデータ要素を格納するカートリッジメモリ CM 数に合わせるように、メインコントローラ39、暗号コントローラ40及び搬送コントローラ41の設定を変更すればよい。

【0072】

さらにまた、暗号化データが記録される第 k 磁気テープカートリッジ MC_k のカートリッジメモリ CM にキーデータが格納されないことを条件に、キーデータそのものを他の磁気テープカートリッジ MC に格納してもよい。このような暗号データ記録・再生方法及び暗号データ記録・再生システムでは、前記したステップ $S11 \sim S16$ (図5中、符号49参照)及びステップ $S20 \sim S35$ (図9中、符号50参照)において、キーデータ要素の読出及び保存をキーデータの読出及び保存に置き換えるとともに、ステップ $S15$ でキーデータを格納する際に、第 k 磁気テープカートリッジ MC_k のカートリッジメモリ CM にキーデータが格納されないように、メインコントローラ39、暗号コントローラ40及び搬送コントローラ41の設定を変更すればよい。

【0073】

そして、これら実施の形態では、キーデータやキーデータ要素を磁気テープカートリッジ MC のカートリッジメモリ CM に格納するライブラリ装置14を例に

として本発明を説明したが、磁気テープカートリッジMCに代えて、フレキシブルディスク、光ディスク、リールに巻回された磁気テープ等の可搬性記録媒体を使用するとともに、キーデータやキーデータ要素をこれら記録媒体のヘッダ部に格納するように本発明を構成してもよい。

【0074】

【発明の効果】

本発明の暗号化データ記録方法、暗号化データ記録システム及び暗号化データ再生システムによれば、キーデータの取り扱いに特段の管理を要することもなく、データの機密保持性が優れ、しかも正当なアクセス権を有する者が容易に暗号化データを復号化して利用することができる。

【図面の簡単な説明】

【図1】

本発明の暗号化データ記録・再生システムの一実施形態として例示するライブラリ装置を備えたコンピュータシステムの構造を概略的に示すブロック図である。

【図2】

ライブラリ装置の構成を例示する斜視図である。

【図3】

アレイに装着された磁気テープカートリッジの様子を示した、一部に切欠き部を含む部分斜視図である。

【図4】

磁気テープカートリッジに搭載されるカートリッジメモリの構造を例示す斜視図である。

【図5】

中央演算処理装置から生データがライブラリ装置に送信されて、キーデータ要素が生成・保存される際のメインコントローラ、暗号コントローラ及び搬送コントローラの動作を例示するフローチャートである。

【図6】

図6(a)は、暗号コントローラで生成されるキーデータ要素のデータ構造を

示す概念図、図 6 (b) は、キーデータテーブルに格納されるキーデータ要素のデータ構造を示す概念図である。

【図 7】

カートリッジメモリに格納されるキーデータ要素のデータ構造及びカートリッジ特定データのデータ構造を示す概念図である。

【図 8】

キーデータを使用して暗号化データを生成する際のメインコントローラ及び暗号コントローラの動作を例示するフローチャートである。

【図 9】

中央演算処理装置から生データを要求する信号がライブラリ装置に送信されて、キーデータ要素をもとにキーデータが生成・保存される際のメインコントローラ、暗号コントローラ及び搬送コントローラの動作を例示するフローチャートである。

【図 1 0】

暗号化データを生データに復号化する際のメインコントローラ及び暗号コントローラの動作を例示するフローチャートである。

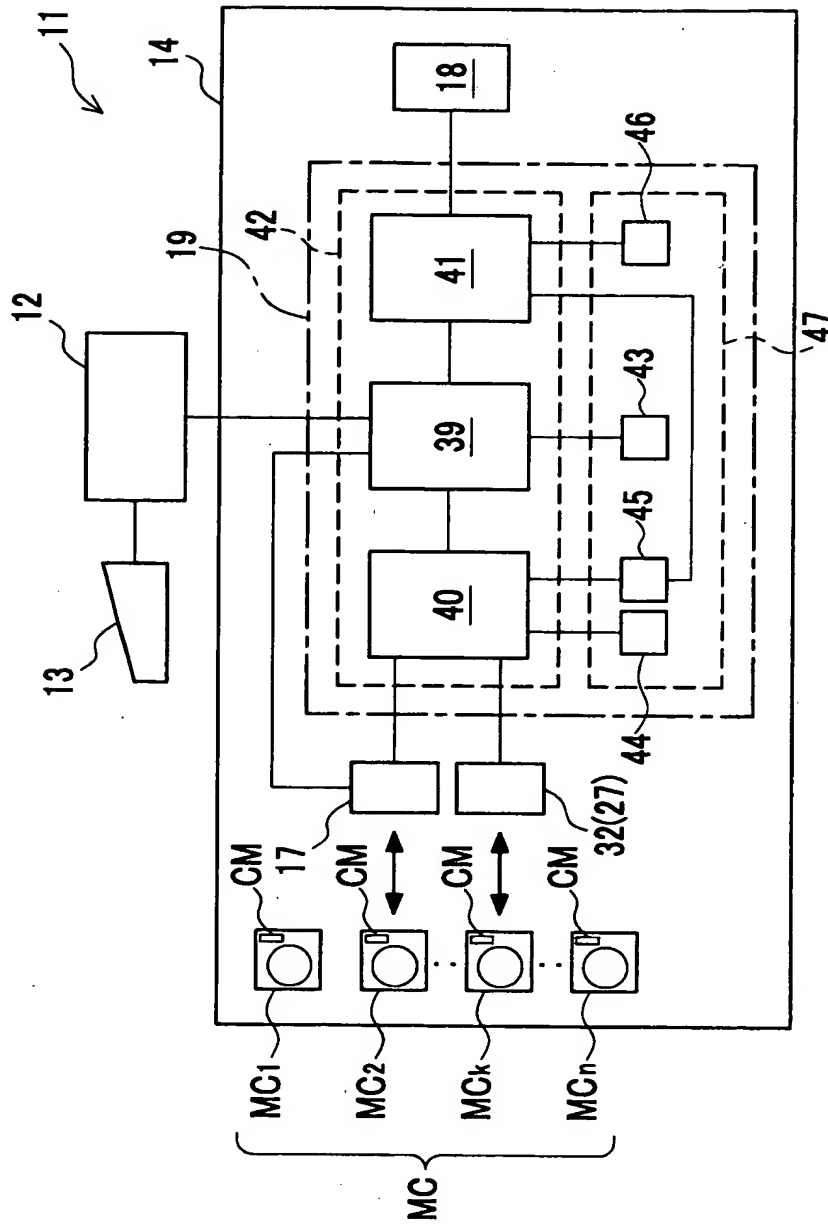
【符号の説明】

- 1 4 ライブラリ装置
- 1 7 ドライブ
- 1 9 制御機構
- MC 磁気テープカートリッジ
- CM カートリッジメモリ

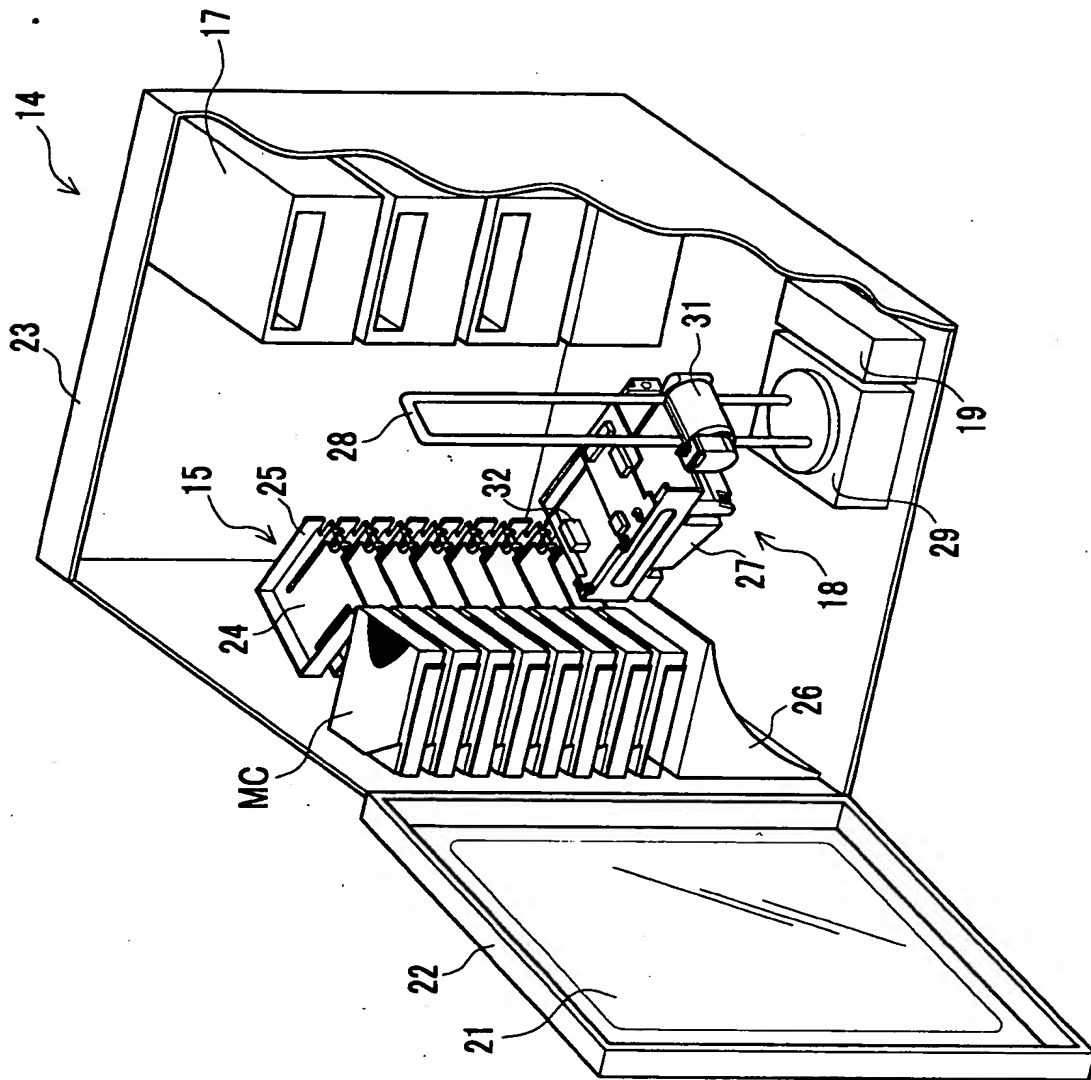
【書類名】

図面

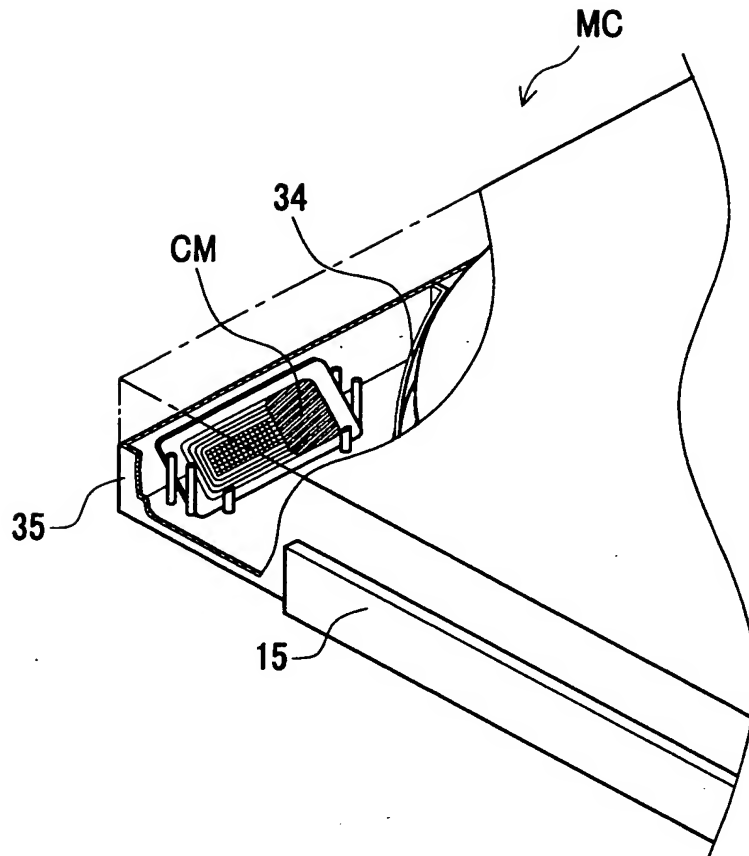
【図 1】



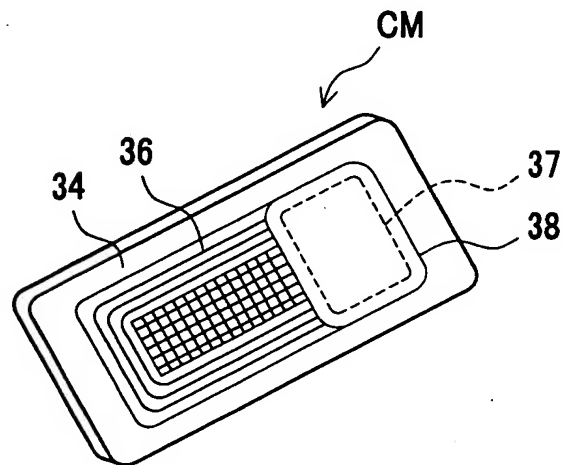
【図 2】



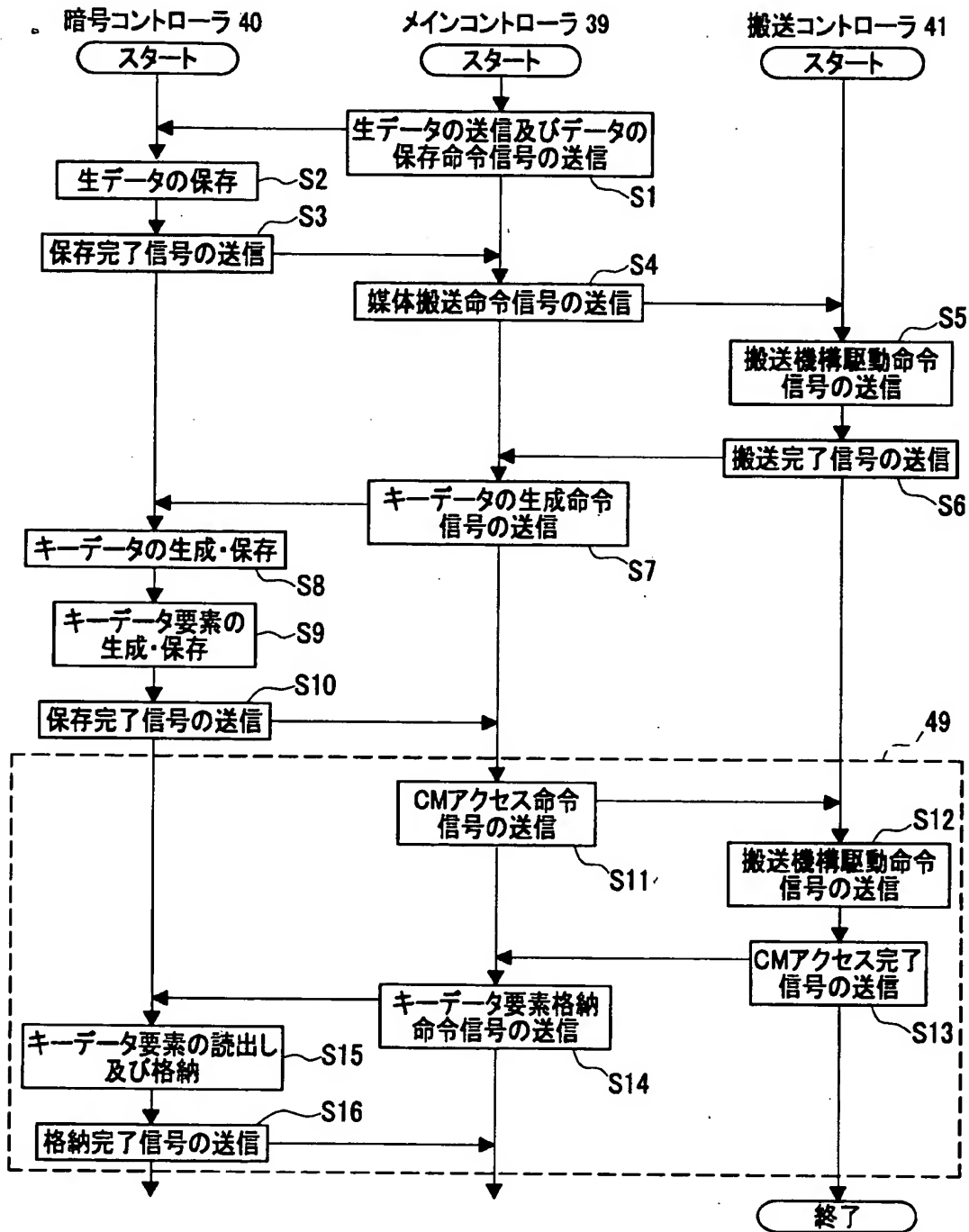
【図 3】



【図 4】

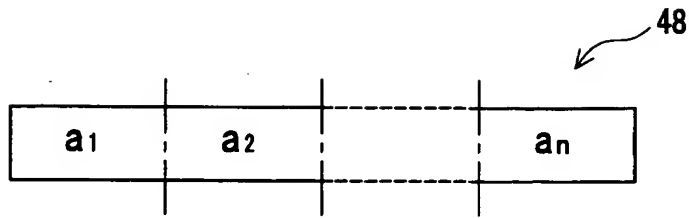


【図 5】

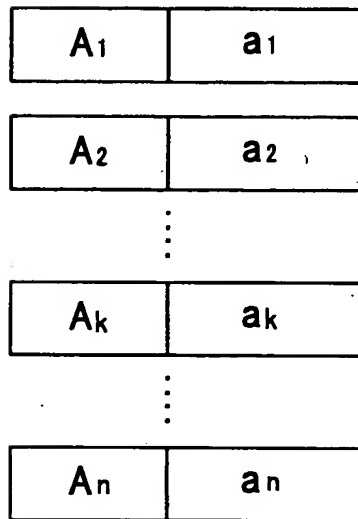


【図 6】

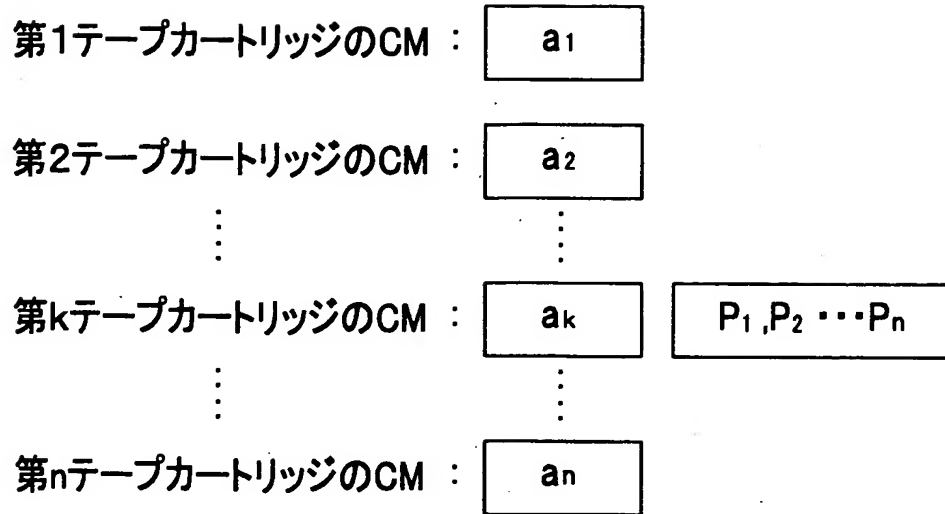
(a)



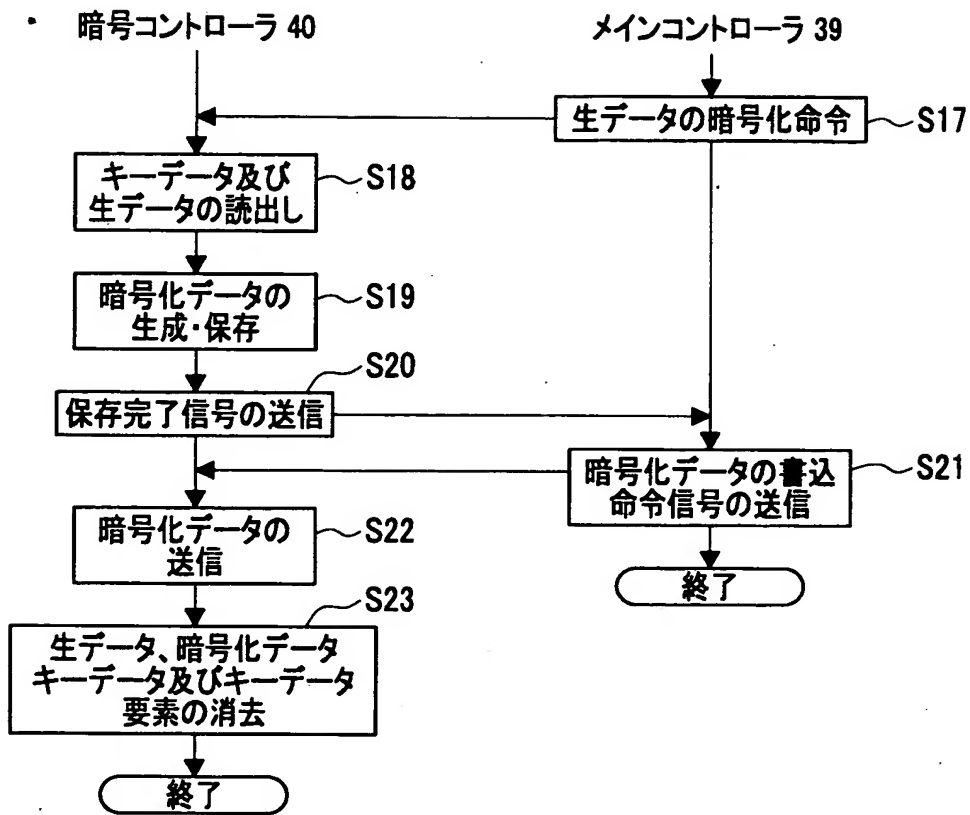
(b)



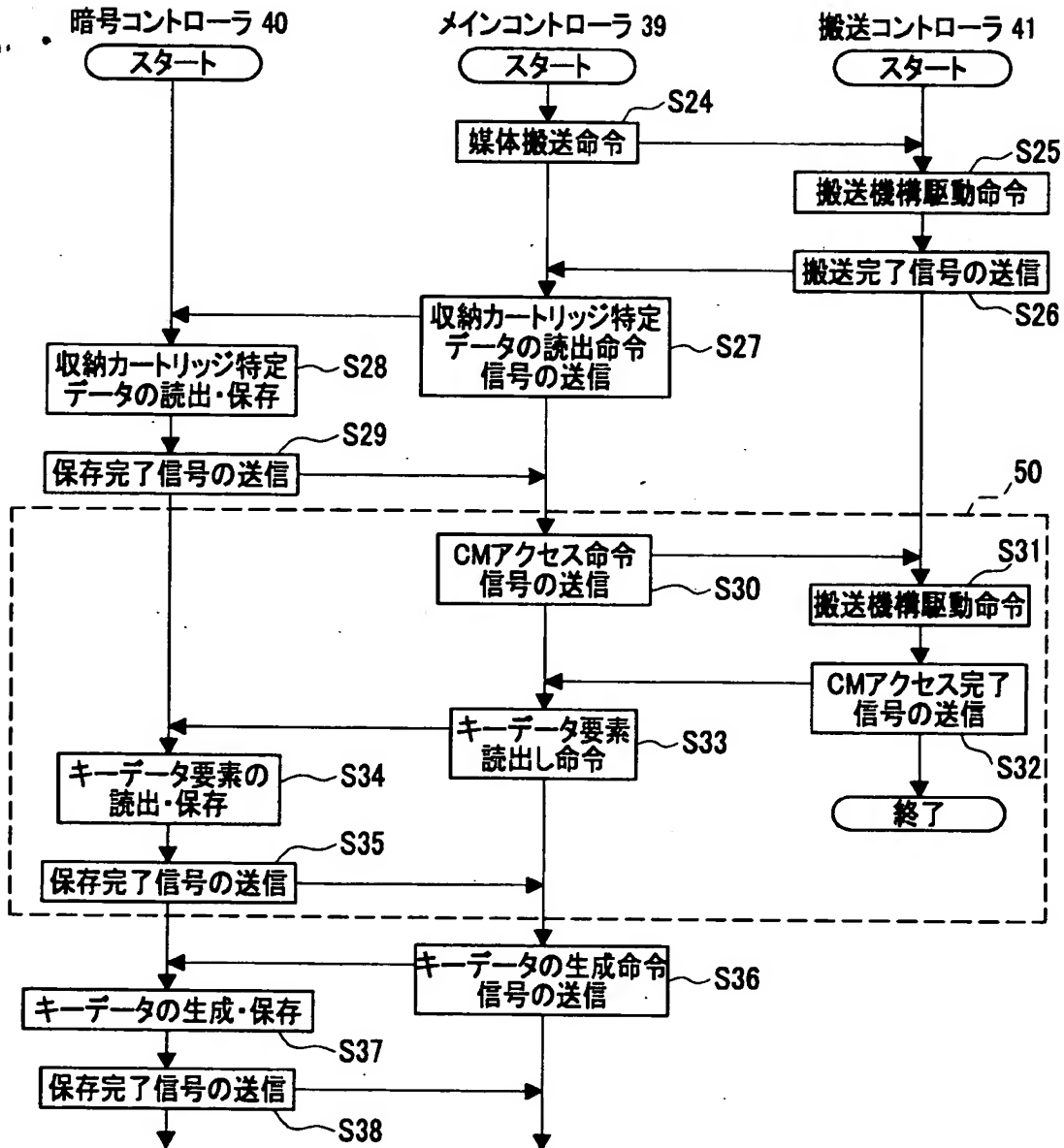
【図 7】



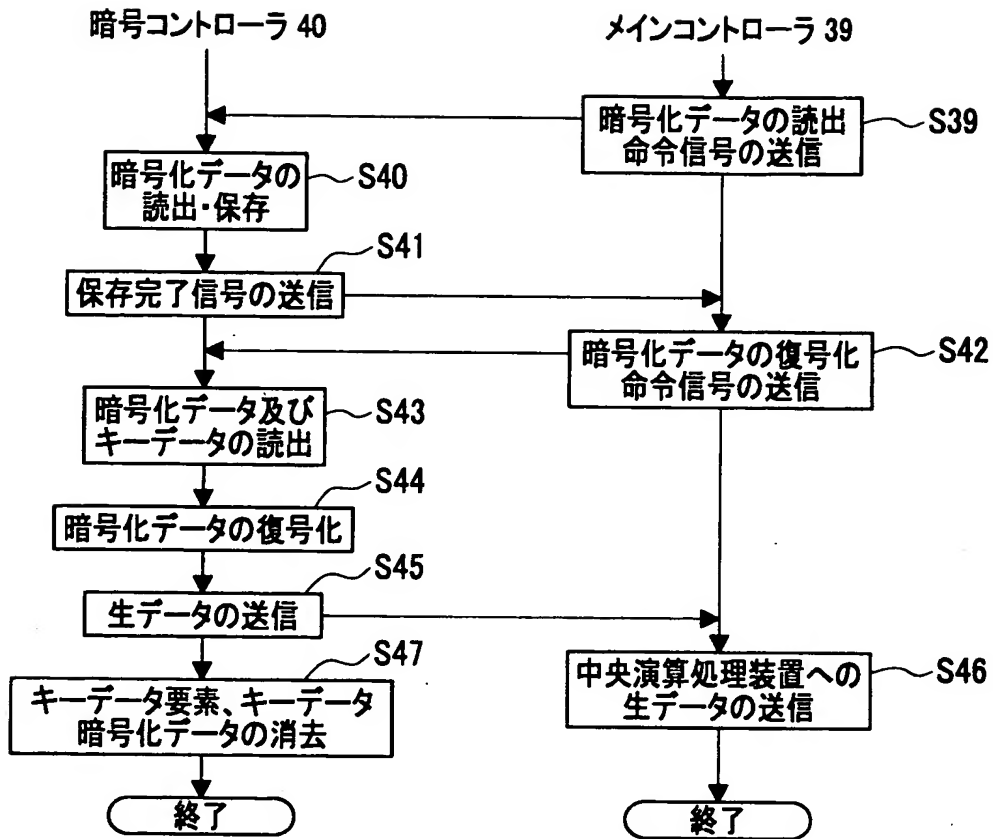
【図 8】



【図 9】



【図 1 0】



【書類名】 要約書

【要約】

【課題】 キーデータの取り扱いに特段の管理を要することもなく、データの機密保持性が優れる暗号化データ記録方法、暗号化データ記録システム及び暗号化データ再生システムを提供する。

【解決手段】 複数の磁気テープカートリッジMCと、前記磁気テープカートリッジMCに暗号化データを書き込むドライブ17と、前記暗号化データのキーデータが分割されたキーデータ要素を格納するカートリッジメモリCMと、前記暗号化データのキーデータを分割して複数のキーデータ要素を生成するとともに、複数の前記キーデータ要素を各カートリッジメモリCMに分けて格納させる制御機構19とで構成する。

【選択図】 図1

出 願 人 履 歴 情 報

識別番号 [000005201]

1. 変更年月日 1990年 8月14日
[変更理由] 新規登録
住 所 神奈川県南足柄市中沼210番地
氏 名 富士写真フイルム株式会社